

Державний вищий навчальний заклад  
«Донецький національний технічний університет»  
Кафедра прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

\_\_\_\_\_ Леонід Бачурін

«\_\_\_\_\_» \_\_\_\_\_ 2023 р.

## РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОНД 2.12 Криптографічні протоколи

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність 125 Кібербезпека  
(шифр і назва спеціальності)

Освітня програма Кібербезпека  
(назва освітньої програми)

Мова навчання: українська

Робоча програма навчальної дисципліни Криптографічні протоколи  
(повна назва дисципліни)  
для здобувачів вищої освіти за спеціальністю 125 Кібербезпека

«6» лютого 2023 року. – 8 с.

Розробник: проф., д.т.н. Ковальчук Л.В.

Робоча програма затверджена на засіданні кафедри Прикладної математики та інформатики  
( назва кафедри)

Протокол №2 від 20.02.2023 р.

В.о. завідувача кафедрою ПМІ к.т.н. доц. Маслова Н.О.

«20» лютого 2023 р.

\_\_\_\_\_  
(підпис) (Маслова Н.О.)  
(прізвище та ініціали)

Схвалено науково-методичною комісією галузі знань 12 Інформаційні технології  
(шифр, назва)

Протокол №1 від 21.02.2023 р.

Голова \_\_\_\_\_ (Башков Є.О.)  
(підпис) (прізвище та ініціали)

## 1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	ОНД- – Обов’язкова навчальна дисципліна	
Обсяг в кредитах ЄКТС	6	
Обсяг в годинах за навчальним планом, разом: в тому числі:	180	
лекції:	48	
практичні заняття:		
лабораторні заняття:	32	
семінари:		
самостійна робота:	100	
Форма підсумкового контролю	Екзамен/диф.залік.	
Курсовий проєкт		
Дисципліну викладають	Викладач: проф. Ковальчук Л.В. e-mail: <a href="mailto:lyudmila.kovalchuk@donntu.edu.ua">lyudmila.kovalchuk@donntu.edu.ua</a> <a href="mailto:lyudmila.kovalchuk@iohk.io">lyudmila.kovalchuk@iohk.io</a> <a href="mailto:lyudmila_kovalchuk@adoriasoft.com">lyudmila_kovalchuk@adoriasoft.com</a>	

**Передумови для вивчення дисципліни:** перелік дисциплін, які мають бути вивчені раніше: Вища математика, Програмування, Теорія ймовірностей та математична статистика Основи інформаційної безпеки, Методи та засоби криптографічного захисту інформації, Інформаційно-комунікаційні системи, Захист операційних систем.

## 2. Мета вивчення навчальної дисципліни

**Метою** вивчення навчальної дисципліни є опанування методами та засобами технічного захисту інформації, підготовка фахівців, здатних розробляти і використовувати технології інформаційної та/або кібербезпеки.

### Загальні компетентності:

- ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
- ЗК 1.Здатність застосовувати знання у практичних ситуаціях.
- ЗК.2. Знання та розуміння предметної області та розуміння професії.
- ФК 2. Здатність до використання інформаційно- комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах
- ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

### **Програмні результати навчання:**

ПК4. аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення

ПК6. критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПК19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах

ПК 47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації

ПК 48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах

### **3. Очікувані результати навчання**

Результатами навчання є оволодіння практичними навичками з проведення процедур криптографічного захисту інформації, застосування криптографічних протоколів, застосування концептуальних знань з навчальних дисциплін загальної підготовки для засвоєння дисциплін професійної підготовки.

В цілому результатами вивчення даної дисципліни є оволодіння методами та засобами технічного захисту інформації, підготовка фахівців, здатних розробляти і використовувати технології інформаційної та/або кібербезпеки.

### **4. Засоби діагностики результатів навчання**

Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня підготовленості студента до виконання конкретної роботи. Форма проведення поточного контролю – усна бесіда за результатами виконання практичних робіт.

Підсумковий контроль проводиться з метою оцінювання результатів навчання та визначається підсумками результатів виконання та захисту практичних робіт по кожній зі змістовних тем.

Підсумковий семестровий контроль – іспит.

### **5. Критерії оцінювання результатів навчання**

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

Лр 1	Лр 2	Лр 3	Лр 4	Лр 5	Лр 6	Лр 7	Лр 8	Поточни й контроль	Екза мен	Макс ималь ний бал
5	5	5	5	5	5	5	5	40	60	100
3	3	3	3	3	3	3	3	24		84

Примітка: 1) Лр1, Лр2 і т.д. практичні роботи;

Сз1, Сз2 і т.д. семінарські заняття;

2) У числівнику максимальний бал – при своєчасному та правильному виконанні, у знаменнику – мінімальний (при правильному, але несвоечасному виконанні)

В оцінку поточного контролю з виконання лабораторних робіт включено контрольні та поточні опитування

Контроль виконання курсового проекту включає поточний контроль за виконанням розрахунків та захист перед комісією. Оцінка виконання та захисту курсового проекту проводиться за 100-бальною шкалою.

### Приклад розподілу балів, які отримують студенти за виконання курсового проекту

Пояснювальна записка	Захист роботи	Сума
40	60	100

Захист роботи має на увазі наявність презентації (10 балів) та доповіді (до 50 балів)

Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»).

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

## 6. Програма навчальної дисципліни

### 6.1. Основні теми дисципліни

Ном. п\п	Назва Лекції //теми	Код
<b>Тема 1. Алгебраїчний апарат, що використовується при побудові криптографічних систем.</b>		
1	<b>Лекція 1.</b> Множини, відображення, операції. Алгебраїчні структури з однією операцією та їх властивості. Теорема Лагранжа.	Л.1/1
2	<b>Лекція 2.</b> Циклічна група та її властивості. Відображення груп, їх властивості.	Л.1/3
3	<b>Лекція 3.</b> Алгебраїчні структури з двома операціями та їх властивості. Характеристика кільця. Мультиплікативна група кільця. Гомоморфізми кілець, їх властивості.	Л.1/5
4	<b>Лекція 4</b> Кільце лишків, його властивості. Мультиплікативна група кільця лишків. Конгруенції та їх властивості. Розв'язування конгруенцій. Квадратичні лишки та нелішки. Обчислення квадратних коренів за модулем	Л.1/7
<b>Тема 2. Симетричні криптосистеми та протоколи.</b>		
5	<b>Лекція 5</b> Симетричні алгоритми шифрування: DES, ГОСТ, інші алгоритми.	Л.2/1
6	<b>Лекція 6.</b> Малоресурсні алгоритми шифрування. Шифр PRESENT. Інші малоресурсні алгоритми.	Л.2/3
7	<b>Лекція 7.</b> Протоколи розподілу секрету, що використовують Китайську теорему про лишки.	Л.2/5
<b>Тема 3. Асиметричні та гібридні криптографічні системи та протоколи.</b>		
8	<b>Лекція 8.</b> Однобічні функції та важкорозв'язувані задачі. Приклади однобічних функцій, їх властивості. Задача факторизації. Задача DLP та задача Діффі-Геллмана, зв'язок між ними.	Л.3/1
9	<b>Лекція 9.</b> Протокол Діффі-Геллмана встановлення спільного ключа. Атаки на протокол. Геш-функції, їх властивості. Алгоритми цифрового підпису.	Л.3/3
10	<b>Лекція 10.</b> Протокол встановлення ключів TLS SSL. Аналіз його складових.	Л.3/5

11	<b>Лекція 11.</b> Гібридний алгоритм встановлення спільного ключа. ДСТУ 9041:2020.	<b>Л.3/7</b>
<b>Тема 4. Протоколи доведення без розголошення.</b>		
12	<b>Лекція 12.</b> Означення протоколу доведення без розголошення. Повнота, коректність, відсутність розголошення, стимулятор, екстрактор. Печера Алі-Баби. Протокол Шнора.	<b>Л.4/1</b>
13	<b>Лекція 13.</b> Протоколи доведення квадратичності та неквадратичності. Протокол доведення знання квадратного кореня у кільці лишків. Протоколи доведення знання значення поліному в точці.	<b>Л.4/3</b>
<b>Тема 5. Протоколи консенсусу, що використовуються у Блокчейн-технологіях.</b>		
14	<b>Лекція 14.</b> Децентралізовані мережі. Спроби створити цифрову валюту та проблеми, що при цьому виникають. Використання геш-функцій для побудови блокчейну.	<b>Л.5/1</b>
15	<b>Лекція 15.</b> Протокол консенсусу Proof-of-Work. Особливості протоколу, його корисні риси та недоліки. Атаки на протокол та способи захисту від атак.	<b>Л.5.3</b>
16	<b>Лекція 16.</b> Протокол консенсусу Proof-of-Stake. Особливості протоколу, його корисні риси та недоліки. Атаки на протокол та способи захисту від атак.	<b>Л.5/5</b>
17	<b>Лекція 17.</b> Інші протоколи консенсусу на блокчейні. Протоколи консенсусу на блокграфах	<b>Л.5/7</b>

## 6.2. Теми практичних (семінарських) занять

Проведення лабораторних занять не передбачено навчальним планом дисципліни

## 6.3. Теми практичних робіт

№ з/п	Назва теми	Кількість годин
1	<b>Лабораторна робота №1 (ЛР 1/2).</b> Розв'язок задач на основні алгебраїчні структури, арифметичні операції та теорему Лагранжа.	4
2	<b>Лабораторна робота №2 (ЛР 1/6).</b> Розв'язок задач на основні властивості циклічних груп. Розв'язок задач на основні алгебраїчні структури з двома операціями та відображення груп і кілець.	4
3	<b>Лабораторна робота №3 (ЛР 2/2).</b> Розв'язок задач на розв'язування конгруенцій та обчислення квадратних коренів за модулем.	2
4	<b>Лабораторна робота №4 (ЛР 2/6).</b> Розв'язок задач на обчислення раундового перетворення алгоритму PRESENT.	4
5	<b>Лабораторна робота №5 (ЛР 3/4).</b> Розв'язок задач на обчислення спільного ключа у протоколі Діффі-Геллмана та на побудову/перевірку цифрових підписів.	4
6	<b>Контрольна робота за Темами 1-3</b>	2
7	<b>Лабораторна робота №6 (ЛР 4/2).</b> Розв'язок задач на використання протоколу Шнора доведення знання експоненти. Побудова стенограми протоколу, побудова екстрактора.	4
8	<b>Лабораторна робота №7 (ЛР 5/2).</b> Розв'язок задач на побудову протоколу розподілу секрету, що використовує Китайську теорему про лишки.	4
9	<b>Лабораторна робота №8 (ЛР 5/6).</b> Розв'язок задач на обчислення імовірності генерації блоків та імовірності успіху атаки подвійної витрати.	2
10	<b>Контрольна робота за темами 4-5</b>	2
...	<b>Усього годин</b>	32

#### 6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	<b>Тема 1.</b> Алгебраїчний апарат, що використовується при побудові криптографічних систем	30
1.1	<b>Тема 2.</b> Симетричні криптосистеми та протоколи	15
1.2	<b>Тема 3.</b> Асиметричні та гібридні криптографічні системи та протоколи.	15
2	<b>Тема 4.</b> Протоколи доведення без розголошення	20
	<b>Тема 5.</b> Протоколи консенсусу, що використовуються у Блокчейн-технологіях.	20
	<b>Усього годин</b>	100

#### 6.5. Індивідуальні та/або групові завдання

У рамках курсу студенти виконують курсовий проект з дисципліни. Тематика роботи: «Побудова оцінок імовірності атаки на протоколи консенсусу Proof-of-Stake та Proof-of-Work для різних параметрів блокчейн-мережі та різних додаткових умовах».

Варіанти завдань обираються згідно номеру в журналі Обліку успішності студентської групи.

Оцінка виконання та захисту курсової роботи проводиться за 100-бальною шкалою.

### 7. Література

#### 7.1. Основна

4. Ковальчук Л.В., Яремчук Ю.Є. Прикладна алгебра. Частина 1. Основи абстрактної алгебри : навчальний посібник / Л.В. Ковальчук, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2015. – 99 с.

2. Вербицький О. В. Вступ до криптології / О.В. Вербицький– Львів: Видавництво науково-технічної літератури, 1998. – 247 с.

3. Л. Ковальчук, С. Конюшок, Н. Кучинська. Прикладна алгебра: основні поняття алгебри та теорії чисел. Навчальний посібник. 2010. 181 стор.

4. Л. Ковальчук, А. Кудін, Н. Кучинська. Математичні аспекти теорії блокчейн. Навчальний посібник. 2022. 141с.

5. ДСТУ 9041:2020 Алгоритм шифрування коротких повідомлень.

6. Koblitz N. Number theory and cryptology. / Cambridge, 1993, 254 p.

7. Justin Thaler. Proofs, Arguments, and Zero-Knowledge. June 27, 2022. 320p.

8. William J. Buchanan, Shancang Li & Rameez Asif. Lightweight cryptography methods. Journal of Cyber Security Technology. Volume 1, 2017 - Issue 3-405 Mar 2018. Pages 187-201.

9. Masanobu Katagi and Shiho Moriai. Lightweight Cryptography for the Internet of Things.

10. A. Bogdanov<sup>1</sup>, L.R. Knudsen<sup>2</sup>, G. Leander<sup>1</sup>, C. Paar<sup>1</sup>, A. Poschmann<sup>1</sup>, M.J.B. Robshaw<sup>3</sup>, Y. Seurin<sup>3</sup>, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. 2007. 18p.

#### 7.2 Допоміжна

11. Leon Groot Bruinderink. Towards Post-Quantum Bitcoin. A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Industrial and Applied Mathematics. 2016. 81p.

12. Kerry A. McKay, Larry Bassham, Meltem Sönmez, Turan Nicky Mouha. NISTIR 8114 Report on Lightweight Cryptography. 2017. 27p.

13. Maksym Petkus. Why and How zk-SNARK Works: Definitive Explanation. 2019. 65p.
14. Харин Ю.С. Математические компьютерные основы криптологии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич – Мн.: Новое знание, 2003. – 382 с.
15. Гапак О.М. Навчальний посібник Криптоаналіз. Криптографічні протоколи. Ужгород, 2021. 82с.

### 7.3. Методична

Методичні вказівки до виконання практичних робіт з дисципліни «Криптографічні протоколи» для студентів денної форми навчання ОС «бакалавр» спеціальності 125 Кібербезпека (планується до видання).

### 8. Інформаційні ресурси

1. Гапак О.М. Посібник з курсу «Компютерна криптографія»  
<https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36505/1/Криптоаналіз.%20Криптографічні%20протоколи.pdf>
2. Криптографічні протоколи, <http://um.co.ua/8/8-2/8-241181.html>